



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Cum

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,020	07/21/2000	Alexandre F. Tenca	245-53434	4090

7590 06/28/2005

Klarquist Sparkman Campbell Leigh & Whinston LLP
One World Trade Center
Suite 1600
121 SW Salmon Street
Portland, OR 97204

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/621,020

Applicant(s)

TENCA ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 March 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 4-10 and 17-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 4,9,10,23,24,26-28 is/are allowed.
- 6) ☒ Claim(s) 5-8,17,18,20-22,25,29 and 30 is/are rejected.
- 7) ☒ Claim(s) 19 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

rd

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed with respect to independent claims 4,5,9,10, and 23 have been persuasive and has found the claim limitations argued to be allowable over the prior art of record.
2. The applicant has argued the rejection of independent claim 5 as being statutory under 35 USC 101. The examiner respectfully disagrees, for it is recited of just software in the current claim language that is not tangibly embodied. The applicant argues that "cryptographic parameters are associated with physical activity, i.e., secure communication between a message sender and a message recipient." The examiner notes that this feature is not claimed by the applicant and the rejection of the claims under 35 USC 101 remains.
3. As per claims 17,20, and 25, the applicant has argued that Monier fails to disclose certain features.

As per claims 17 and 25, it is argued by the applicant that Monier fails to disclose of an intermediate value. The applicant has claimed the limitation, however there is no use of the limitation claimed, hence it is not applied in the Montgomery multiplication process until dependent claim 19. If the applicant were to add all the limitations of dependent claim 19 into claim 17, it would be allowable over the prior art of record.

As per claim 20, the applicant argues that Monier fails to disclose of inputs to receive words of the first operand and modulus. The examiner respectfully disagrees,

Monier discloses of inputs for receiving the operands and modulus, please refer to col. 3, lines 47-50.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 5-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims currently recite of software alone and of itself and do not fall into a statutory class. It is suggested by the examiner that the claims be amended to include a computer readable medium containing instructions for performing Montgomery multiplication/product as is recited in the respective dependent claims.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 17,18,20-22,25, and 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Monier et al. The examiner notes that the applicant's claim language is bracketed next to the prior art's similar limitations.

As per claim 17, the teachings of Monier et al disclose of a circuit (apparatus) for performing Montgomery multiplication of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words of the multiplicand (first operand), words of the modulus, an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45). A control unit is also shown in Figure 1 that is situated and configured to direct words of the multiplicand (first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

As per claim 18, Figure 1 of Monier et al also demonstrates of a data path along which words of the multiplicand (first operand) and multiplier (second operand) are delivered to the processing elements (col. col. 3, lines 38-49).

As per claim 20, the teachings of Monier et al disclose of a circuit for performing Montgomery multiplication (product) of a multiplicand (first operand) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words of the multiplicand (first operand), words of the modulus, an output that delivers values of words of the Montgomery multiplication (product)(col. 3, lines 38-45 and col. 4, lines 12-45). Monier et al also demonstrates in Figure 1 of a data path along which words of the multiplicand (first operand) and multiplier (second operand) are delivered to the processing elements (col. col. 3, lines 38-49).

As per claim 21, Monier et al recites of inputs for receiving words of the multiplicand (first operand), an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second operand)(col. 3, lines 38-45 and col. 4, lines 12-45).

As per claim 22, Figure 1 demonstrates of a data path configured to provide a first selected bit of the multiplier (second operand) to the first processing element and a second selected bit of the multiplier (second operand) to a second processing element (col. 3, lines 38-45 and col. 4, lines 12-45).

As per claims 25 and 30, the teachings of Monier et al disclose of a circuit (apparatus/smart card) for performing Montgomery multiplication of a multiplicand (first cryptographic parameter) and a multiplier (second operand) with respect to a modulus (col. 3, lines 38-49). Figure 1 shows a plurality of processing elements that includes inputs for words (messages) of the multiplicand (first operand), words of the modulus, an intermediate value of a word of Montgomery multiplication (product), and an input for a bit of the multiplier (second cryptographic parameter)(col. 3, lines 38-45 and col. 4, lines 12-45). A control unit is also shown in Figure 1 that is situated and configured to direct words of the multiplicand (first operand), words of the modulus, and bits of the multiplier (second operand) to the processing elements (col. 3, lines 38-49 and col. 4, lines 12-45).

Allowable Subject Matter

8. Claim 19 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.


Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

June 26, 2005

Christopher Revak
AU 2131


6/26/05